Les libertés comme fondement de la protection des données nominatives

Poullet, Yves

Published in:
La vie privée : une liberté parmi les autres ?

Publication date:
1992

Document Version
le PDF de l'éditeur

LES LIBERTÉS COMME FONDEMENT DE LA PROTECTION DES DONNÉES NOMINATIVES (1)

I. — INTRODUCTION

1. Dans un article récent (2) nous montrions combien la thèse de F. Rigaux sur la nature et l'essence du « droit » à la vie privée conçu non sur le mode d'un droit réel mais comme l'expression de libertés permettait d'éclairer d'un jour nouveau le fondement des législations de protection des données.

Le présent article approfondit la réflexion. Dans une première partie (I) nous nous efforcerons de montrer comment les principes fondamentaux des lois relatives aux traitements de données à caractère personnel (droit d'accès, principe de finalité, autorité de contrôle) participent à la construction d'un système de protection à la recherche d'un équilibre entre des intérêts et/ou libertés qui s'opposent. Nous verrons dans le même temps qu'un tel système permet seul d'offrir une réponse adéquate à une évolution technologique en pleine ébullition.

Dans une seconde partie (II), nous nous demanderons sur quelle base les autorités de contrôle, et le cas échéant le juge, peuvent garantir et contrôler rationnellement une pondération d'intérêts qui permette tant l'éclosion d'un marché de l'information fondé sur la libre circulation des données que la protection des libertés individuelles. Certes, cet arbitrage ne peut s'opérer qu'à propos de situations particulières, toujours spécifiques, mais n'existe-t-il pas — et la thèse du professeur Rigaux nous y conduit — une « méthode », une « règle méthodologique » générale permettant aux autorités de contrôle d'exercer leurs missions avec rigueur et transparence ? Nous chercherons alors

(1) Nous tenons à remercier tout particulièrement Mlles M.-H. Boulanger, C. de Terwangne et M.-N. Willockx ainsi que M. X. Thunis pour leurs réflexions critiques et enrichissantes.

(2) Y. POULLET, « Le fondement du droit à la protection des données nominatives : « propriétés ou libertés » », in *Nouvelles technologies et propriété*, LITEC, 1991, p. 175 à 205.

une piste de solution dans l'application de la règle de proportionnalité au contrôle du principe de finalité. Cela nous permettra ensuite de relativiser la distinction, traditionnelle dans les législations « privacy », entre les secteurs public et privé. Nous verrons alors que la « méthode » proposée implique une vision nouvelle de la portée du consentement de l'individu concerné par les données.

II. — Du droit à l'autodétermination aux libertés

A. — *Généralités*

2. Un jugement déjà ancien du Tribunal constitutionnel fédéral allemand va nous permettre de mieux apprécier la thèse du professeur Rigaux selon laquelle la vie privée est à comprendre comme un lieu de libertés et non pas comme l'objet d'un droit subjectif classique.

Les « Verts », parti écologiste, introduisent un recours devant le Tribunal constitutionnel contre la loi relative au recensement démographique et ses mesures d'exécution. Un jugement du 15 décembre 1983 leur donne raison. Il ordonne de compléter le programme d'enquête statistique de certaines mesures procédurales et de sécurité et déclare inconstitutionnelle la communication des données collectées. Le fondement de la décision est l'atteinte aux « droits généraux de la personnalité » progressivement dégagés par le tribunal fédéral allemand sur base des articles 1[er] (1) (intangibilité de la dignité humaine) et 2 (1) (droit à l'épanouissement de la personnalité) de la Loi fondamentale allemande. Le Tribunal fédéral considère le « droit à l'autodétermination en matière d'information » (*Informationnelle Selbstbestimmungsrecht*) comme partie intégrante des droits généraux de la personne humaine : « La valeur et la dignité de la personne humaine agissant librement comme membre d'une société libre sont les principes essentiels de la loi fondamentale » (3).

(3) H. Burkert, *Datenschutz und Informations- und Kommunikationstechnik : Eine Problemskizze*, Bonn, G.M.D., 1985.

3. Ce droit à l'autodétermination, qui est le droit de tout individu à maîtriser l'image qu'il donne de lui-même dans la société doit être protégé des risques d'abus résultant des possibilités actuelles et futures de traitements automatisés de l'information. Il ne peut cependant s'entendre de façon absolue. Comme l'a souligné la Cour constitutionnelle : « L'individu n'exerce pas une souveraineté absolue sur les faits le concernant ; sa personnalité se développant au sein d'une communauté sociale, il ne peut vivre sans communiquer. L'information, même si elle est nominative, est une représentation de la réalité sociale, qui n'est pas uniquement la propriété de l'individu concerné (...). La Loi fondamentale résout la dichotomie individu-société en considérant la personne comme une entité liée et insérée dans la société. C'est pourquoi en principe, l'individu doit accepter des restrictions de son 'droit à l'autodétermination en matière d'information' et ce, en faveur de l'intérêt général prépondérant » (4).

4. Ainsi, le droit à l'autodétermination constituerait le véritable fondement de la législation de protection des données. Mais, en définitive, qu'est-ce que ce droit à l'autodétermination sinon une liberté, selon l'expression du professeur Rigaux (5) ?

La thèse de Rigaux est précisément de démontrer que la protection de la vie privée et au-delà des biens de la personnalité se rattache directement à la liberté de l'individu et que toute confusion ou comparaison avec les droits subjectifs patrimoniaux classiques obscurcit le débat. « Devant les biens de la personnalité s'ouvre un champ infiniment plus vaste que celui qui y a été assigné jusqu'ici. Il ne s'agit certes pas de doubler tous les droits patrimoniaux d'un ectoplasme qualifié de droit de la personnalité, mais plutôt de réajuster dans leur ensemble les règles applicables à ces droits d'une manière qui prenne mieux en considération la dignité et la personnalité des agents juridiques privés » (6).

(4) BVerfG., EUGRZ, 1983, 588. Cet arrêt a fait de l'objet de nombreux commentaires ; outre celui de H. Burkert (« Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », *D.I.T., Droit de l'informatique et des télécommunications*, 1985, 8-16), on citera celui de S. Simitis, « Das Informationelle Selbstbestimmungsrecht, Grundbedingung einer Verfassungskonformen Informationsordnung », *NJW* 1984, 398-404.

(5) F. Rigaux, *La protection de la vie privée et les autres biens de la personnalité*, Bruylant-L.G.D.J., Bruxelles-Paris, 1990, p. 758, n° 684.

(6) *Idem*, p. 763, n° 685.

Selon l'auteur, le droit à la protection des données ne peut se comprendre en réduisant le débat à la reconnaissance d'un droit subjectif qualifié de droit à la vie privée.

Les droits subjectifs se caractérisent en effet par le fait qu'ils confèrent à leur titulaire l'appartenance maîtrise d'un objet déterminé : « Il appartient à la nature de ces droits de conférer à leur titulaire des prérogatives précises accompagnées d'un droit d'exclusivité » (7). « Existe-t-il une 'sphère privée' qui ferait l'objet d'une appropriation exclusive du sujet et, en tant que telle, soustraite à toute immixtion de tiers ? La maîtrise de cette sphère privée est-elle protégée par un droit subjectif inconditionnel analogue au droit de propriété ? L'impossibilité de circonscrire cette sphère autrement que par une définition tautologique impose de donner à ces questions une réponse négative. La recherche d'un noyau dur qu'on appellerait 'intimité de la vie privée' n'est pas moins vouée à l'échec. Même les atteintes les plus graves, qu'on peut présumer illicites et qui ont généralement ce caractère le perdent dans des circonstances exceptionnelles. Il arrive que les membres de la société civile aient intérêt à être informés de faits qui appartiennent (...) à la vie intime du sujet ou que celui-ci ne puisse se prévaloir d'un intérêt assez contraignant pour résister à pareille divulgation dont l'auteur fait alors un usage qui n'est pas illicite de sa propre liberté » (8).

B. — *Approfondissements et implications en matière de protection des données*

5. La thèse de Rigaux met en évidence les points suivants :

a) La liberté et la dignité humaine, fondement ultime des législations de protection des données, justifient, eu égard au danger particulier lié au traitement automatique des données, la consécration de droits subjectifs précis, permettant aux individus d'avoir les moyens minima d'exercer leurs droits à l'autodétermination. Selon la Cour constitutionnelle allemande : « Face au danger déjà décrit de l'usage du traitement automatique de l'information, le législateur doit prendre de plus amples mesures qu'auparavant quant à l'organisation et à la procédure d'un

(7) *Idem*, p. 768, n° 687.
(8) *Idem*, p. 770, n° 687.

traitement de données et ce, afin d'empêcher toute violation du droit de la personne humaine (...) » (9).

Dans cette perspective, serait justifiée la consécration de droits subjectifs particuliers que l'on pourrait rassembler sous la qualification de droit d'accès. L'analogie avec le droit à la paternité, droit subjectif particulier né des attributs non patrimoniaux conférés à l'auteur, peut être évoquée à ce propos. Il s'agira de montrer que ce droit subjectif peut prendre de nouvelles formes, eu égard aux dangers nouveaux ou aux particularités de nouvelles techniques.

b) La liberté et la dignité humaine affrontent d'autres libertés, celles d'autrui, d'autres intérêts et notamment l'intérêt général.

« Liberté plutôt que droit, le *Selbststimmungsrecht* doit se concilier avec la liberté également reconnue à tous les autres sujets de droit. Les droits fondamentaux sont parfois en conflit avec les uns et les autres. Enfin et surtout, le Bundesverfassungsgericht n'a pas reconnu au droit à l'épanouissement de la personnalité, une portée absolue. Chaque fois qu'elle l'estime nécessaire, la juridiction constitutionnelle a rappelé que l'individu est une personne insérée dans la société : celle-ci peut, dans l'intérêt général ou pour la protection des droits d'autrui, imposer aux citoyens des devoirs ou des abstentions qui empêchent leur liberté naturelle » (10). « Ainsi, la liberté de la vie privée protège le sujet contre l'expropriation d'un bien de la personnalité par l'Etat et contre l'appropriation d'un tel bien par un autre citoyen » (11). Les législations de protection des données entendent définir certains critères qui permettront de préciser ce droit à l'information du ficheur, expression tantôt de sa liberté d'entreprendre, dans le secteur privé, tantôt de son rôle de gardien de l'intérêt général, dans le secteur public.

c) Enfin, la thèse de Rigaux souligne la nécessité de définir de façon évolutive l'équilibre des intérêts en conflit et oblige

(9) BVerfG., EUGRZ, 1983, 588.
(10) F. RIGAUX, *La protection de la personne et de la vie privée*, Louvain, U.C.L., Faculté de droit, 1988, p. 485.
(11) F. RIGAUX, *supra*, *Cinquième leçon : La doctrine des droits de la personnalité*, n° 134.

d'approfondir le rôle des institutions chargées en premier lieu d'aider à la définition de cet équilibre dans ce contexte évolutif.

Chacun de ces points fait l'objet de commentaires particuliers.

a) *Des droits subjectifs nouveaux*

1° *Explication et contenu*

6. Rigaux écrit : « Dans l'Etat social moderne, l'intangibilité de la dignité humaine ne saurait plus être garantie selon le modèle aujourd'hui dépassé de Locke : liberté et propriété. Ce serait trop dire que les droits nouveaux ont été conçus contre la propriété, mais ils exercent une fonction de complément ou de substitut. Pour que le droit de propriété reste tolérable, avec les considérables inégalités qu'il a entretenues, force a été d'instituer tantôt des droits subjectifs nouveaux, tantôt l'illusion de tels droits » (12).

Le droit d'accès sous ses multiples facettes reconnu au fiché ne peut-il être, dans cette perspective, considéré comme un droit subjectif nouveau, c'est-à-dire comme le complément ou plutôt le corollaire rendant tolérable le surcroît de puissance que confère le traitement automatisé de données à celui qui les détient ? La modification d'ordre tant quantitatif que qualitatif de la valeur informationnelle de la donnée nominative, modification obtenue par le traitement informatique de même que la non-transparence des circuits d'information exigent la reconnaissance pour le fiché de droits subjectifs nouveaux, rassemblés sous le vocable de « droit d'accès ».

7. En résumé, le droit d'accès peut se définir comme le droit de la personne fichée à participer à la formation de l'image que les personnes qui l'entourent se font d'elle. Ce droit ne nécessitait pas la consécration de droits subjectifs particuliers dans les sociétés traditionnelles où la circulation de l'information nominative pouvait aisément se contrôler. Il en est tout autrement dans nos sociétés actuelles.

(12) F. RIGAUX, *La protection de la vie privée et les autres ..., op. cit.*, p. 753, n° 679.

Un exemple tiré de la vie quotidienne suffit à le démontrer : jusqu'il y a peu, le paiement au comptant représentait la forme habituelle de paiement. La valeur informationnelle d'un paiement au comptant est quasi nulle et le vendeur sauf s'il connaît l'identité de son acheteur peut difficilement établir une corrélation entre tel individu et telle dépense. En toute hypothèse, l'acheteur identifié peut connaître *a priori* les personnes (voisins) à qui l'information sera transmise. Dans le cas de l'utilisation d'un terminal point de vente, le paiement acquiert une valeur informationnelle sans commune mesure avec celle relevée pour le paiement au comptant. Ainsi, l'utilisation du terminal renseigne le banquier (tiers à la transaction) sur l'identité non seulement de l'acheteur mais également du commerçant, l'importance de la transaction voire sa nature. Le commerçant obtient une information sur la relation bancaire de son client et sur sa valeur de crédit. L'utilisation de systèmes informatiques pour la gestion de telles informations accroît encore leur valeur informationnelle puisque le recoupement des informations primaires obtenues, leurs comparaisons permettront rapidement à leurs détenteurs de se faire une image précise des habitudes de consommation d'un client, de ses déplacements et de l'importance relative de chacune de ses dépenses. « Même les goûts culturels et artistiques par le biais des librairies et des salles de spectacle fréqentées deviennent soudainement transparents. Bref, à travers chaque transaction économique, l'usager d'une carte de crédit révèle à un tiers qui ne lui demande pas son avis, sa personnalité, ses projets et ses dépenses futures compte tenu de sa situation sociale globale » (13).

8. Classiquement, nos législations d'Europe occidentale ont envisagé le droit d'accès sous de multiples facettes :

— d'abord, lors de la collecte d'informations, c'est le droit pour le fiché de savoir pourquoi on l'interroge, le caractère obligatoire ou non de la réponse, de connaître l'utilisateur et la finalité d'utilisation de l'information ;
— également, le droit pour le public en général de connaître, par l'existence d'un fichier des fichiers, le degré d'informati-

(13) J.-P. LEMASSON, « Les cartes de paiement : la privatisation de la vie privée », *Technologies de l'information et société*, 1988, n° 1, p. 113.

sation d'une société, les relations entre les fichiers, leur concentration, etc. ;

— ensuite, encore que nombre de nouvelles législations abandonnent ou restreignent ce droit, le droit pour chaque individu de savoir qu'il est fiché, afin de lui permettre dans un second temps, de connaître les données de base (et non les données résultat) figurant à son propos dans le fichier informatisé ;

— enfin, il s'agit pour le fiché de pouvoir exiger, par des procédures rapides et le cas échéant avec l'aide de l'autorité chargée de la protection des données, la rectification, l'effacement de certaines données auprès du ficheur voire auprès de tiers en relation avec celui-ci.

2° *Evolution du droit d'accès*

9. Si le droit d'accès est un ensemble de droits subjectifs nouveaux correctifs d'un droit de propriété auquel les nouvelles technologies de l'information donnent un pouvoir que l'on peut craindre excessif, certains développements actuels de ces nouvelles technologies, dans la mesure où ils accentuent encore l'absence de maîtrise par l'individu des circuits d'information le concernant, conduisent certains à compléter par de nouveaux droits subjectifs le droit d'accès tel qu'il avait été consacré par les législations de protection des données. En effet, le progrès technologique a créé de nouveaux modes de collecte de l'information. Ceux-ci sont plus insidieux parce que moins transparents, plus automatiques puisque liés à l'utilisation d'un service télématique, et enfin plus dangereux car en liaison avec l'utilisation d'un service d'intérêt général comme le téléphone. Deux débats relayés par les autorités de protection des données, l'un surtout allemand à propos des nouveaux compléments au service téléphonique offerts par le R.N.I.S. (14), l'autre en France, à propos des cartes à mémoire utilisées dans le domaine de la santé, illustrent cette évolution du droit d'accès.

(14) Réseaux Numériques à Intégration de Services. A cet égard, Y. POULLET, F. WARRANT, « Nouveaux compléments aux services téléphoniques et protection des données : la recherche d'un cadre conceptuel », *D.I.T.*, 1990, n° 2, 18-25.

10. A propos des nouveaux compléments du service téléphonique offerts dans le cadre du R.N.I.S., la discussion qui eut lieu dans l'ex-R.F.A. a mis en évidence la nécessité de promouvoir une information préalable de l'abonné au service téléphonique afin que celui-ci puisse exercer son *consentement* éclairé concernant diverses options rendues possibles par la technologie du réseau à intégration de services, ainsi l'identification du numéro de l'appelant, la facturation détaillée, la figuration du nom de l'abonné et de ses qualités dans l'annuaire électronique.

Le *droit à la transparence* des circuits d'information consiste essentiellement dans l'obligation pour l'opérateur, pour toute personne intervenant dans l'exécution du service et pour le serveur, d'informer l'abonné des enregistrements, traitements, stockages et cessions de données nominatives le concernant, et ce préalablement à leur collecte. Ce droit à la transparence se double d'un droit au *consentement libre et éclairé* de l'abonné à différents stades : lors du prélèvement des données nominatives, ce sera le droit de ne pas figurer dans l'annuaire et d'exiger la non-divulgation du numéro d'abonné ; ce sera également le droit d'exiger ou de refuser l'envoi automatique de facturations détaillées, la non-visualisation de son numéro sur le terminal appelé. Enfin, pointe une légitime revendication complémentaire des deux premières, celle du *droit à l'anonymat*, le droit d'exiger que soient mises en œuvre des techniques (par exemple, les cartes préchargées anonymes) permettant l'utilisation anonyme d'un service d'intérêt général comme le téléphone.

11. L'insertion d'un microprocesseur dans des cartes à mémoire a suscité certaines recommandations de la CNIL française prises dans le cadre d'expériences de cartes « Santé ». Trois principes les éclairent :

— *celui du volontariat* : patients et médecins ne peuvent être contraints de participer à la mise en œuvre d'un système informatisé de traitement des données. Aucun avantage ni aucune pénalisation ne peuvent être la conséquence d'un refus de participation ;

— *celui du consentement libre et éclairé à l'usage de la carte* : patients et médecins doivent être clairement informés des finalités et modalités du système, des modes d'inscription ou d'effacement des informations contenues dans la carte à

mémoire, des personnes habilitées à lire ces informations et des garanties, droits et recours dont ils disposent ;

— *celui enfin de l'exclusion de toute discrimination* : le principe du libre choix du médecin par le patient et le principe du choix de la pratique médicale ne peuvent être remis en cause d'une manière ou d'une autre.

Ainsi, la création de nouveaux modes de collecte, de dissémination et de conservation de l'information peut élargir la signification du droit d'accès conçu comme toute mesure visant à permettre au fiché de maîtriser les circuits par lesquels transite l'information le concernant.

b) *Les incidences du principe de finalité sur le droit à l'information des ficheurs et ses limites*

1° *Principes*

12. Puisque l'individu n'est pas propriétaire des données le concernant, ni même titulaire sur elles d'un droit proche d'un droit réel, puisque c'est de façon spontanée que l'individu projette dans la société une certaine image de lui, cette image précisément peut être captée par autrui, rapprochée d'autres informations et prendre ainsi un sens aux yeux de celui qui la traite. Il ne peut être question *a priori* de nier à autrui, le droit d'utiliser l'image que je donne de moi-même. A ma liberté, s'oppose la sienne qu'il s'agisse de la liberté d'association dans le cadre de traitements opérés par un syndicat, de la liberté religieuse dans le cadre de traitements gérés par l'autorité religieuse ou plus fréquemment de la liberté d'entreprendre dans le cas de fichiers d'entreprises. Ce conflit de libertés doit se résoudre par la *méthode de pondération des intérêts* par laquelle l'autorité chargée de trancher le conflit appréciera les intérêts légitimes respectifs propres à chaque partie exprimant sa liberté.

Nous reviendrons sur ce point mais notons d'emblée que nombre de prescrits législatifs prévoyant une exception pour certaines données ou certains traitements s'expliquent de la sorte. Si les législations interdisent le traitement de données philosophiques, syndicales ou religieuses, c'est qu'*a priori* le traitement de telles données met en péril ma liberté du même nom ; que toujours à propos de ces mêmes données, les mêmes législations exemptent de cette interdiction précisément les associations religieuses ou syndicales voire la presse, s'explique par la volonté d'affirmer la prééminence de la liberté d'association, de la presse sur les libertés individuelles.

13. Comme le montrent ces exemples limités, l'enregistrement de la même donnée nominative sera tantôt interdit, tantôt réglementé, tantôt libre suivant les libertés mises en cause par son enregistrement. Il y a bien débat entre libertés et nécessité d'apprécier au regard des intérêts de la société le poids accordé à chacune d'elles.

En ce qui concerne précisément la liberté d'entreprendre du ficheur, peut-on admettre, au-delà des limites imposées à l'égard de certaines données qui caractérisent de façon immédiate des libertés constitutionnelles reconnues (liberté d'opinion, de religion, d'association), qu'une législation définisse en même temps que le droit à l'information du ficheur, les limites de ce droit ? Le principe de la liberté du ficheur de collecter des données ne doit-il pas être affirmé en tant que tel quitte à ce qu'*a posteriori*, certains abus soient réglés au cas par cas par le juge ? En d'autres termes, une législation de protection des données doit-elle intervenir vis-à-vis des traitements du secteur privé autrement qu'en prévoyant un droit d'accès (15) et notamment réglementer le contenu et les limites des traitements privés ? La réponse à cette question peut être élucidée par l'étude des principes de la réglementation des traitements du secteur public.

2° *Application aux secteurs public et privé*

14. Le droit de l'autorité publique à collecter les données et à les traiter ne peut s'expliquer par une liberté fondamentale qui justifierait en soi ce droit. La décision du Bundesgerichtshof déjà citée explicite comme suit le bien-fondé de ce droit et en tire des conséquences : « Comme la jurisprudence du Tribunal fédéral constitutionnel l'a mis à plusieurs reprises en évidence, la Loi fondamentale résout la dichotomie individu-société en considérant la personne comme une entité liée et insérée dans la société (...). C'est pourquoi, en principe, l'individu doit accepter des restrictions de son 'droit à l'autodétermination en matière

(15) Voir *supra*, n°s 7 et svts.

d'information' et ce, en faveur de l'intérêt général prépondérant »(16).

Selon la Cour allemande, ces restrictions du droit à l'autodétermination nécessitent cependant un fondement légal conforme à la Constitution et leur énoncé doit respecter les principes de clarté des normes et de proportionnalité. En ce qui concerne le traitement électronique de l'information, cela signifie concrètement que « face au danger déjà décrit de l'usage du traitement automatique de l'information, le législateur doit prendre de plus amples mesures qu'auparavant quant à l'organisation et à la procédure d'un traitement de données, et ce, afin d'empêcher toute violation du droit de la personne humaine (...) »(17).

15. Le droit à l'information des autorités publiques, indispensable pour assurer un service public efficace, et les restrictions du droit à l'autodétermination qu'il implique ne peut s'exercer que dans le respect de *trois principes, ceux de légalité, de spécialité et de proportionnalité*. Ces trois principes ont la signification suivante :

— *le principe de légalité* exige que toute banque de données soit créée sous le contrôle du législatif, c'est-à-dire que les principaux éléments de la réglementation soient définis par une loi au sens formel du terme. De façon générale, ce principe implique une certaine coordination et un certain contrôle par le législatif de l'informatisation du secteur public. Au-delà du problème des libertés individuelles, le principe de légalité permet de préserver l'équilibre des pouvoirs. L'utilisation croissante de l'informatisation dans le secteur public renforce en effet les pouvoirs d'action de l'exécutif et modifie l'équilibre des pouvoirs, garant institutionnel de la démocratie. Le rattachement de l'autorité de contrôle de protection des données au législatif et le large droit de saisine accordé au législatif auprès de cette autorité participent également au rééquilibrage des pouvoirs ;

— *le principe de spécialité* exige que le législateur indique avec précision les objectifs de l'utilisation des données nominatives et les destinataires des ou de certaines des données collectées. Ainsi, chaque autorité administrative ne peut enregistrer des données que dans le cadre de la mission qui lui a été confiée et pour autant que cela soit nécessaire à sa réalisation. En toute hypothèse, l'autorité administrative doit choisir la voie la moins coûteuse en termes de restriction des libertés de l'administré ;

— *le principe de proportionnalité* implique, quant à lui, que les traitements mis sur pied par l'autorité administrative au nom de l'intérêt général ou de la protection des intérêts des citoyens n'engendrent pas une restriction disproportionnée des libertés individuelles.

(16) BVerfG, EUGRZ, 1983, 589.
(17) H. BURKERT, *Op. cit.*, p. 9.

Ces deux derniers principes ont pour conséquence qu'au sein des administrations : « Il faut veiller à ce que des traitements dont la collecte et l'utilisation poursuivent des finalités différentes ne soient pas interconnectés. Il faut s'assurer ensuite que chaque domaine distinct de l'activité de l'administration reste bien séparé et ce par une interdiction de communiquer entre ces secteurs d'activité : le pouvoir exécutif devrait ainsi veiller à créer des domaines informationnels cloisonnés (...) Le principe général de la séparation des pouvoirs serait en conséquence complété (à l'intérieur de l'administration) par une 'séparation des pouvoirs en matière d'information' » (18).

16. Concernant le secteur privé, les législations de protection des données d'Europe occidentale ont consacré des principes parallèles à ceux développés pour le secteur public. Elle peut surprendre l'observateur nord-américain qui exclut les traitements du secteur privé du champ d'application des législations de protection des données. Cette application analogique des mêmes principes fondamentaux tous secteurs confondus s'explique par le fait que l'Etat déborde son rôle constitutionnel traditionnel : « A son devoir traditionnel d'abstention, simplement accompagné de l'obligation générale de maintien de l'ordre, s'ajoute désormais le devoir de prendre les mesures requises pour la sauvegarde des droits fondamentaux auxquelles appartient aussi une réglementation satisfaisante des rapports juridiques privés » (19). Cette extension du rôle de l'Etat justifie la

(18) *Idem*, note 32, p. 12.
(19) F. RIGAUX, *op. cit.*, pp. 681 et 682, n° 607.

consécration explicite ou implicite dans les législations d'Europe occidentale du principe de finalité (20) applicable aux fichiers du secteur privé et parallèle aux principes déjà décrits en ce qui concerne les fichiers du secteur public.

17. Dans le secteur privé, « le service attendu de l'entreprise collectrice des données est à la fois la justification et la limite de l'usage des renseignements » concluait déjà le rapport TRICOT (21). Le principe de finalité déduit du rapport contractuel est repris par les lois allemande, autrichienne, danoise, norvégienne et néerlandaise.

A ce stade du raisonnement, nous nous contenterons de quelques réflexions générales, nous réservant (voir *infra*, n^os^ 36 et svts) le soin de revenir plus amplement sur la double signification de ce principe.

A la base de la nécessaire consécration de ce principe, repose la constatation suivante : « Il ne faut pas perdre de vue que c'est toujours dans un but bien déterminé que les données sont rassemblées, mises en mémoire et communiquées. C'est seulement lorsqu'on connaît cet objectif et non en raisonnant dans l'abstrait sur l'information elle-même que l'on peut tracer la limite de tolérance acceptable pour l'intéressé » (22).

Certains objecteront l'imprécision du principe. La notion de « finalité », disent-ils, est singulièrement floue et son emploi crée le risque d'une interprétation fort large. La critique nous apparaît peu fondée. Le respect du critère de la « finalité » est en effet plus souple et plus respectueux d'une appréciation judiciaire évolutive que le critère *a priori*, réglementaire, tiré de la nature soi-disant « en soi » des données, critère qui, par opposition, est peu soucieux de la réalité contractuelle.

18. Le « droit à l'information » des entreprises et de l'administration entraîne pour elles certaines conséquences relatives à l'utilisation de ces données.

(20) Sur la portée exacte du principe de finalité, voir II, *infra*.

(21) *Rapport Informatique et Libertés* de la Commission « Informatique et Libertés » instituée par le décret n° 74-438, du 8 novembre 1974 (*J.O.*, 13 novembre 1974), Paris, La documentation française, 1975, T. I, p. 106.

(22) *Idem*, pp. 45 et svtes.

Elles sont responsables de la sécurité de leurs fichiers. L'article 7 de la Convention du Conseil de l'Europe (23) mentionne : « Des mesures de sécurité appropriées sont prises pour la protection des données contre la destruction accidentelle ainsi que contre l'accès, la modification ou la diffusion non autorisés ».

Cette question de sécurité exige :

— la consécration de règles déontologiques applicables à toutes les personnes qui ont à approcher les banques de données ;
— pour les centres de traitement localisables, la nomination de « gestionnaires », c'est-à-dire des personnes chargées au sein des entreprises et administrations du respect de la réglementation de l'information dont le statut doit être proche de celui des commissaires-réviseurs ;
— la définition progressive de normes de sécurité nationales et internationales pour les programmes traitant de données nominatives.

Le droit à l'information des entreprises ou administrations doit être soigneusement distingué du droit de communication. « La règle posée ci-dessus, à savoir le principe de pertinence, explique le rapport TRICOT, implique que les renseignements possédés par une entreprise et recueillis à l'occasion d'un contrat particulier ne doivent pas être diffusés à des tiers » (24). Ainsi, selon la section 28 (1) de la loi allemande, une entreprise n'a droit à la communication de données venant d'une autre entreprise qu'à la condition qu'elle soit conforme dans le chef de la seconde entreprise au but contractuel à la base du traitement des données, mais en outre qu'elle soit justifiée dans le chef de la première par la protection d'intérêts légitimes dans son chef ou dans le chef d'un tiers.

3° *Incidence de l'évolution technologique*

19. L'évolution des technologies a notamment pour caractéristique de permettre aux entreprises de trouver chaque jour des applications, par la combinaison de programmes existants, par

(23) Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *Série des Traités européens*, Janvier 1981, n° 108.

(24) Rapport TRICOT, *op. cit.*, p. 48.

la définition de nouvelles applications, par le choix de nouvelles clés pour structurer telle ou telle base de données, par l'ajout d'un champ d'interrogation dans une banque de données ; ainsi une banque fournissant hier un relevé de compte des débits du client peut proposer demain dans le cadre du même service une aide à la gestion des budgets des ménages en indexant chaque dépense en fonction de rubriques telles consommation de carburant, dépenses d'acquisitions de biens et services, virement à des tiers, etc. Il est clair que, ce faisant, de nouvelles finalités du traitement apparaissent. Ce n'est pas le lieu de juger de leur bien-fondé mais simplement de faire remarquer qu'il sera de plus en plus difficile de circonscrire une fois pour toutes la finalité des traitements et que des systèmes réglementaires fondés sur des déclarations ou des autorisations *a priori* des finalités auront sans doute quelques difficultés à prendre en compte cette évolution permanente des finalités rendue possible par les technologies modernes.

Le fondement même de la réglementation des traitements informatiques traitant des données nominatives justifie que le principe de finalité puisse être apprécié différemment, étant donné les risques nouveaux suscités par les développements récents de la technologie. Deux exemples suffiront : les systèmes experts et les traitements opérés dans le cadre d'opérations télématiques dites « grand public ».

α Principe de finalité et systèmes experts

20. Le développement des systèmes d'intelligence artificielle ou des systèmes experts suggère quelques réflexions relatives au principe de finalité. Ces systèmes figent dans une procédure automatisée un raisonnement humain : ainsi, un système expert permettra d'évaluer la solvabilité d'un demandeur de crédit ou de déduire certaines informations complémentaires à partir de données minimales relatives à un consommateur ou un groupe de consommateurs.

Il est traditionnel de rappeler à propos de tels systèmes la règle énoncée par l'article 2 de la loi française suivant laquelle « aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé » (25).

Deux réflexions complémentaires doivent être faites. Premièrement, l'utilisation de systèmes experts pour identifier non point simplement des individus mais bien des groupes d'individus justifierait l'extension du prescrit aux traitements relatifs à des groupes d'individus. Secondement, il serait utile que l'intéressé qui a lieu de craindre l'utilisation (ou la mauvaise pondération) par le système expert de paramètres non pertinents (par exemple, l'origine (lieu de naissance) de la personne comme critère d'évaluation de sa dignité au crédit) puisse en saisir l'autorité de contrôle. Ajoutons que celle-ci ne pourrait intervenir qu'en cas d'abus flagrants (dans l'exemple donné, pondération aberrante donnée au critère de lieu de naissance dissimulant une discrimination raciale), sous peine de constituer une restriction inacceptable à la liberté d'entreprise. Cette dernière implique en effet que le responsable du traitement puisse fonder ses décisions sur des critères qu'il choisit de privilégier en fonction de ses objectifs propres et de sa connaissance du marché. Cette réflexion à propos du secteur privé nous amène à des conclusions différentes dans le secteur public, où la transparence des critères retenus par les systèmes experts et leur pondération nous apparaissent une condition de leur utilisation.

β Principe de finalité et services télématiques grand public

21. L'analyse de prescrits réglementaires en projet — ainsi, l'EFT Privacy Act américain — ou déjà adoptés relatifs à des *services télématiques* conduit à d'autres réflexions toujours relatives à l'application du principe de finalité. La première, la plus importante, met en évidence la définition *a priori* par la réglementation des types de traitements permis à ceux qui offrent de tels services. Ainsi, l'article 9 du Bildschirmtextvertrag allemand, applicable aux services videotex grand public, prescrit que le serveur ne peut traiter les données que pour des besoins de sa facturation et de connaissance statistique de la clientèle. Il interdit la cession des données à des tiers et la constitution

(25) Article 2 de la loi (française) n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

d'un profil type client, sauf accord de ce dernier. Il limite la durée de conservation des données.

Cette tendance à définir *a priori* le contenu des données pertinentes, la durée de leur conservation et les types de finalités légitimes peut heurter certains, favorables à la définition libre par l'entreprise, maître du fichier, des finalités des traitements opérés, et à réserver un contrôle *a posteriori* au juge ou à un organisme chargé de contrôler le respect de la légitimité des finalités du traitement. Ce principe d'un contrôle *a posteriori* a été adopté dans bien des législations, en particulier allemande, autrichienne, danoise, norvégienne, etc. La remise en cause du principe en matière de services interactifs grand public nous semble procéder des craintes renforcées provoquées à la fois par la nature des données enregistrées et leur mode de collecte.

22. La deuxième réflexion s'attache à l'interdiction de proposer certains services télématiques, ainsi l'exclusion du service de sondage à domicile. Dans le même esprit, devraient être interdits certains traitements, ainsi le traitement des données créées par l'utilisation à distance de jeux video, dans la mesure où leur traitement permettrait la connaissance de la psychologie de l'utilisateur.

23. La troisième réflexion concerne la distinction opérée entre, d'une part, les partenaires au service — celui qui offre le service et celui qui reçoit le droit de l'utiliser — et, d'autre part, les intervenants à la réalisation du service, ce qu'en matière de T.E.F. (26), le projet américain (l'EFT Privacy Act) qualifie de « EFT Service Provider », c'est-à-dire en l'occurrence les commerçants chez qui des terminaux sont installés, les centres serveurs communs à différents prestataires de services, les transporteurs, etc.

La réglementation des traitements opérés par cette seconde catégorie d'acteurs est plus sévère. Leur droit au stockage des données dans le cadre de leur mission est strictement limité ; leur sont interdites non seulement la commercialisation des données mais également la constitution de pool de renseignements qui pourraient être utiles aux membres du réseau. Se retrouve

(26) Transferts Electroniques de Fonds ou Electronic Fund Transfer.

ici la distinction opérée dans certaines législations (par exemple, les législations allemande, autrichienne, danoise) entre les entreprises traitant des données pour le compte d'autrui, soumises à une réglementation plus rigoureuse (régime d'autorisation), et les autres.

c) *Le rôle des autorités de protection des données*

24. Définissant l'approche réglementaire souhaitable de la technologie informationnelle, le professeur Burkert parlait de « learning systems », c'est-à-dire d'une solution législative qui, dans le cadre d'un système réglementaire, établit « an institution provided with competence to collect the information in the regulated area, to make ad-hoc decisions according to rather more generally formulated criteria in a law and to feed back the information collected during the execution of its tasks to society and its rule making agencies » (27).

Ainsi, le système est capable d'apprendre et de s'adapter, concluait l'auteur. Il est clair que le rôle attribué par nos législations d'Europe occidentale aux autorités de protection des données correspond à ce souhait. Ces autorités ont de multiples rôles : « Chien de garde pour assurer la légitimité des actions de ceux qui collectent, traitent et distribuent l'information (rôle exécuté soit par la voie d'autorisations générales ou spécifiques et/ou à travers un pouvoir d'investigation) ; organe consultatif pour le secteur public et parfois également pour le secteur privé, un de ses buts étant de promouvoir des pratiques convenues ensemble en mettant en place des règles relatives à la circulation de l'information ; une institution de règlement ou de solution de litiges ; un organe avec des pouvoirs indépendants pour créer des normes et disposant d'une compétence pour adapter les principes affirmés par la loi » (28).

25. Cette conception des législations dites « privacy » et le rôle central attribué à l'autorité de protection des données cadrent parfaitement avec l'analyse proposée : la réglementation de protection des données ne se résume-t-elle pas dans un débat,

(27) H. BURKERT, « The Dimensions of information law », *La Télématique*, Gand, Story-Scientia, 1985, T. I, p. 214.

(28) S. RODOTA, « The Social Challenge of Information Technology, 1984 and beyond », *Colloque de l'O.C.D.E.*, Berlin, Nov. 28-30, 1984, Inédit.

celui que nous évoquions, entre libertés, la liberté du ficheur et celle mise en péril par la liberté du ficheur, la liberté du fiché ? Ce débat ne peut être résolu une fois pour toutes. Sa solution exige que l'autorité chargée d'arbitrer ce débat puisse peser les intérêts en jeu et ce, au regard d'une évolution technologique qui interdit de figer les solutions mais oblige à apprécier combien celle-ci modifie les équilibres fragiles à peine définis (29).

26. Ainsi, le rôle essentiel des autorités de protection des données est d'être un lieu de dialogue et de négociation. En France, le système des normes simplifiées discutées avec les représentants d'un secteur met en œuvre de façon souple et non contraignante une réglementation adaptée aux particularités du secteur en question. La solution de la récente législation hollandaise et la pratique du Data Protection Act s'inspirent du même principe lorsqu'elles permettent au secteur d'élaborer des codes de conduite dont la ratification est par la suite négociée avec la commission de protection des données. Il nous paraît que ce nouveau rôle des autorités de protection des données est indispensable et doit être élargi. Le risque existe cependant de voir l'arbitrage faussé au profit des responsables de traitements qui, défendant une position commune, se retrouveraient seuls à la table des négociations. A cet égard, la transparence des débats et la représentation des fichés sont capitales afin que l'autorité de protection des données soit une pièce maîtresse du dialogue entre ficheur et fiché et contribue à définir une société informationnelle plus conviviale.

III. — Pondération des intérêts et règle de proportionnalité : incidences sur le principe de finalité

27. La première partie de cette étude a souligné comment les intérêts de la personne concernée par les données s'opposaient à ceux de la personne responsable du traitement. Il a été dit à plusieurs reprises que ce conflit devait se résoudre par la

(29) Cfr *supra*, l'évolution du droit d'accès promue par les autorités de protection des données (n°s 10 et svts) et *infra*, quant au mode d'appréciation du principe de finalité (n°s 40 et svts).

méthode de pondération des intérêts. Dans un premier point (A), nous tenterons de cerner en quoi consiste cette méthode. Dans un second point (B), il sera précisé comment celle-ci s'applique en matière de traitements de données à caractère personnel.

A. — *Pondération des intérêts et règle de proportionnalité*

28. D'une manière générale, pondérer les intérêts désigne plutôt le but à poursuivre lors de l'analyse d'un conflit de libertés que la démarche à suivre pour y arriver. Notre propos est précisément d'éclairer cette dimension importante de la question. La règle de proportionnalité dégagée par une doctrine récente nous y aidera.

En effet, la « méthode » de pondération des intérêts, mise en exergue par le professeur Rigaux, vise, on l'a vu, à résoudre un conflit qui oppose soit deux libertés fondamentales, soit une liberté fondamentale et l'intérêt général. Dans le premier cas, elle conduit à soupeser les intérêts en concours, et dans le second, à « évaluer la restriction qu'il est justifié d'apporter à une liberté individuelle en raison d'une nécessité sociale » (30). Dans notre matière, le conflit qui doit être résolu peut prendre une double signification. Dans le secteur privé, un intérêt ou une liberté, la plupart du temps économique, se heurte aux libertés des personnes concernées par les données. Par exemple, au nom de sa liberté d'entreprendre, une association regroupant différentes banques met sur pied un fichier commun reprenant des informations recueillies par chacun des membres sur les clients considérés comme « mauvais payeurs ». Dans le secteur public, les libertés des personnes concernées sont mises à mal au nom de l'intérêt général. Il suffit ici de rappeler que les polices du monde entier mettent en œuvre des fichiers rassemblant quantité de données relatives aux personnes dont les activités sont de nature à porter atteinte à la sûreté de l'Etat (31).

(30) F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, *op. cit.*, p. 18, n° 6.

(31) Voir par exemple l'avis de la C.N.I.L. du 17 mai 1983 relatif aux fichiers mis en œuvre par la D.S.T., repris in J. Huet et H. Maisl, *Droit de l'informatique et des télécommunications*, Litec, Paris, 1989, p. 228.

Pondérer les intérêts est un exercice périlleux dès lors qu'aucune démarche systématique n'est proposée au juge ou à l'autorité de contrôle afin de guider leur raisonnement.

Prôner la pondération des intérêts ne revient qu'à cerner le résultat à atteindre. Ce faisant, on ne rend pas compte du double contrôle préalable à toute recherche d'équilibre. Comment équilibrer deux libertés (intérêts, etc.) sans poser dès le départ la question du lien de causalité entre les moyens que l'on met en œuvre et la liberté (ou l'intérêt) dont on se prévaut ? Comment également ne pas vérifier si la restriction apportée à la liberté de la vie privée est réellement nécessaire à l'expression pleine et entière de la liberté ou de l'intérêt qui provoque cette atteinte (32) ?

Pareille absence de démarche logique et systématique garantissant formellement la validité de l'équilibre retenu comme solution, peut susciter un sentiment de méfiance par le trop grand pouvoir d'appréciation laissé à ceux qui ont pour mission de contrôler la correcte application du principe de finalité. On peut craindre en effet que, suivant l'humeur du moment, la pression des événements, le fléau de la balance penche tantôt à droite, tantôt à gauche. D'où le besoin de munir le juge et l'autorité de contrôle d'un certain nombre de critères qui leur permettent d'assurer, à la suite d'une démarche rationnelle, le respect d'un équilibre entre les libertés ou/et les intérêts en présence.

29. Afin de fixer des limites au pouvoir d'appréciation de ceux qui ont pour mission d'appliquer le principe de finalité, on peut, à la suite d'une réflexion de M. Van Gerven (33), tenter de rechercher l'équilibre des intérêts en appliquant la règle de proportionnalité. L'auteur a très bien montré comment celle-ci, utilisée depuis longtemps en droit économique européen, se retrouve *mutatis mutandis* dans la problématique de la protection des droits fondamentaux. Avant d'entrer plus avant dans

(32) Le professeur Rigaux relève d'ailleurs qu'aux États-Unis comme dans le système constitutionnel allemand, « l'atteinte portée à une liberté fondamentale doit être limitée à ce qui est strictement nécessaire, soit pour donner satisfaction à l'intérêt général, soit pour assurer la protection d'un intérêt privé » (*op. cit.*, n° 600).

(33) W. VAN GERVEN, « Principe de proportionnalité, abus de droit et droits fondamentaux », *J.T.*, 1992, pp. 305 à 309.

l'argumentation, il convient de rappeler en quoi consiste la règle de proportionnalité.

30. L'application de la *règle de proportionnalité* implique un triple examen (34), qu'elle porte sur la légitimité d'une atteinte par un particulier à un droit ou une liberté d'autrui (35) ou sur un acte déterminé pris dans l'exercice d'une compétence (36). Le premier concerne le contrôle de l'utilité de l'acte ou des moyens mis en œuvre. Il s'agira de vérifier s'ils présentent un lien de causalité suffisant avec l'objectif poursuivi. Le second vise le caractère indispensable des mesures prises ou envisagées, eu égard au fait qu'elles ne peuvent être remplacées par d'autres mesures qui permettraient d'atteindre le même objectif avec une efficacité identique tout en étant plus respectueuses de la liberté, de l'intérêt ou du droit ainsi énervé. Le troisième s'assurera que l'atteinte aux libertés impliquée par les mesures prises n'est pas disproportionnée par rapport au but poursuivi.

31. Il est à remarquer que ce triple examen procède d'une démarche purement formelle qui n'empiète en rien sur le fond de la décision. La personne investie du pouvoir de contrôle garde la pleine maîtrise de ses choix. Ceci donne à la règle de proportionnalité une très grande souplesse qui permet son utilisation dans des hypothèses très variées. La règle peut par exemple être utilisée lorsqu'il s'agit de contrôler la restriction apportée par une loi nationale à un droit protégé par un instrument international (37) ou par une constitution (38). Elle permet aussi d'apprécier un abus de droit (39), la légitimité d'une atteinte contractuelle à un droit fondamental d'une des par-

(34) Sur son application par la Cour de justice européenne, voir les conclusions de l'avocat général W. VAN GERVEN dans l'affaire Eurim-Pharma, C-347/89, *Rec.*, p. 1760.

(35) W. VAN GERVEN, *op. cit.*, pp. 307 à 309.

(36) *Idem*, pp. 305 et 306.

(37) Voir les articles 8 à 11 de la Convention européenne des droits de l'homme.

(38) Par exemple le contrôle exercé par notre Cour d'arbitrage concernant le respect des articles 6 et 6*bis* de la Constitution. Pour plus de précisions, consulter W. VAN GERVEN, *op. cit.*, pp. 305 à 307 ; aussi J.-P. COSTA, « Le principe de proportionnalité dans la jurisprudence du Conseil d'État (de France) », *A.J.D.A.*, 1988, pp. 434 et svtes ; P. VAN OMMESLAGHE, « Abus de droit, fraudes aux droits des tiers et fraude à la loi », note sous Cass., 10 sept. 1971, *R.C.J.B.*, 1976, pp. 303 et svtes, spéc. n^{os} 12 et svts.

(39) W. VAN GERVEN, *op. cit.*, p. 307.

ties (40) ou celle d'une atteinte résultant d'un « acte qui n'est pas un acte juridique » (41).

32. La règle de proportionnalité dote le juriste d'un ensemble de critères formels d'appréciation de la restriction qui est apportée à un droit, une liberté ou un intérêt protégés. Elle peut être utilisée en cas d'opposition entre deux droits (ou libertés, etc.) jouissant d'une protection juridique équivalente ou non.

Si ces droits ou libertés sont protégés par des normes de hiérarchie égale, l'application de la règle de proportionnalité prolonge le principe selon lequel l'exercice d'un droit ou d'une liberté trouve sa limite dans celui ou celle qui est exercé(e) par autrui. On en trouve une illustration en droit belge dans la théorie de l'abus de droit, spécialement en ce qui concerne le droit de propriété. Si la restriction est effectuée au nom d'une liberté ou d'un intérêt protégé par une norme hiérarchiquement inférieure, l'application du principe de proportionnalité se fonde sur le fait que, comme le rappelle fort à propos le professeur Rigaux, « aucune liberté et aucun droit subjectif civil n'ont dans l'État de droit une valeur absolue (...) Ils se laissent tous mesurer à la force des intérêts publics ou privés avec lesquels ils entrent en concours » (42). Ainsi une loi ordinaire peut très bien restreindre l'exercice d'une liberté fondamentale protégée par la Constitution au nom de l'intérêt général ou pour la protection d'un intérêt privé (43).

(40) *Idem*, p. 308.

(41) *Idem*, pp. 308 et 309.

(42) F. RIGAUX, *op. cit.*, n° 591.

(43) Voir F. RIGAUX, *op. cit.*, n° 590. Remarquons avec M. Rigaux que le principe de hiérarchie des normes n'est pas remis ici en cause (cfr n°s 590 et 591). Il s'applique bel et bien même si c'est d'une manière incidente. L'objet des normes en présence est en effet particulier. Les libertés et intérêts invoqués ont par essence un objet indéterminé, à géométrie variable. Pour déterminer s'il existe un conflit entre la norme supérieure et la norme inférieure, il faut cerner le champ d'application matériel respectif des libertés et intérêts qui s'opposent. Or, cette analyse supposera toujours que soit déterminée l'étendue de l'objet de la liberté de la vie privée en fonction de celui de l'intérêt ou de la liberté (voire du droit) qui lui est opposé. Pour ce faire, il faut obligatoirement pondérer les intérêts. Si l'on constate un déséquilibre, on applique la norme supérieure, qui, par hypothèse, est la règle qui reconnait la liberté de la vie privée. Si l'on constate que l'équilibre est préservé, il faut conclure à l'inexistence d'un conflit entre les normes.

33. Loin de se confondre avec le but vers lequel tend la *pondération des intérêts* (44), la règle de proportionnalité guide le raisonnement de celui qui cherche à découvrir si l'équilibre des intérêts est respecté. A chaque niveau d'analyse — utilité, nécessité et proportionnalité — celui qui est investi de la mission de contrôle est amené à affiner son approche de l'équilibre à atteindre. Ainsi comprise, la *méthode de pondération des intérêts* consiste en une application de la règle de proportionnalité en vue de cerner l'équilibre à atteindre.

Cette méthode consiste dans une première étape à se demander si les moyens mis en œuvre sur base d'un intérêt, d'une liberté ou d'un droit se justifient au nom de ceux-ci. Autrement dit, est-ce légitimement que l'on se prévaut de telle liberté ou de tel intérêt ? Dans la deuxième étape, l'interprète recherche s'il est possible de suivre une autre voie, tout aussi efficace, mais qui évite — ou du moins restreint — l'atteinte à la vie privée. Les réponses positives apportées à ces deux premiers examens lui permettront d'évaluer dans quelle mesure la liberté, le droit ou l'intérêt invoqués s'opposent aux libertés mises en exergue lorsque l'on parle de défense de la vie privée. Dans une troisième étape, l'autorité investie du pouvoir de contrôle examinera si le résultat obtenu compense l'ingérence provoquée dans la vie privée de l'individu ou, en d'autres termes, si l'immixtion ne rompt pas l'équilibre entre les intérêts contradictoires.

34. Les avantages de cette méthode de pondération des intérêts apparaissent clairement (45). Elle est systématique et complète ; le raisonnement acquiert ainsi une assise méthodologique. Le jugement de valeur posé par l'autorité de contrôle acquiert une transparence qui réduit l'indétermination de la pondération en tant que telle. Le risque de subjectivité diminue également car

(44) Le professeur Rigaux semble d'ailleurs séparer soigneusement les deux (voir ainsi le n° 609 où l'auteur souligne que la Cour européenne applique fréquemment la méthode de pondération mais qu'*en outre*, elle s'assure du respect de la proportionnalité ; voir aussi les n°s 592 à 600 où les deux problèmes sont distingués).

(45) Voir W. VAN GERVEN, « Principe de ... », *op. cit.*, p. 309 où l'auteur conclut en des termes qui peuvent se transposer très exactement à notre problématique : « (...) l'application du principe de proportionnalité n'offre pas de solutions toutes prêtes. Elle présente néanmoins le mérite, selon nous, que des problèmes délicats, sujets à controverse dans la société, peuvent être abordés d'une manière sereine dans un cadre de référence communément admis, permettant ainsi de motiver la solution retenue et de la fonder sur des arguments contrôlables. »

le triple examen implique une exigence de motivation des plus appréciables. Enfin, cette transparence est un gage de confiance pour les justiciables et le public en général, mieux à même de comprendre les décisions qui sont portées à leur connaissance.

B. — *Application de la méthode de pondération des intérêts en matière de protection des données nominatives*

35. Comme nous l'avons vu (n^os^ 12 et svts), c'est essentiellement par le biais du principe de finalité que la méthode de pondération des intérêts est mise en œuvre en matière de traitement de données à caractère personnel. Attachons-nous à comprendre comment la méthode de pondération des intérêts peut être appliquée au contrôle du principe de finalité (a). L'emploi de cette méthode tant dans le secteur privé que public permettra alors de relativiser cette distinction (b). Nous verrons finalement que l'utilisation de la méthode de pondération des intérêts permet d'éclairer sous un jour nouveau la portée du consentement de la personne concernée (c).

a) *Le contrôle de la finalité*

1° *Principes*

36. Un traitement de données à caractère personnel est toujours créé pour atteindre un certain résultat. Ainsi, une banque décide-t-elle de traiter des données à caractère personnel concernant ses client afin de gérer leurs comptes. Seul le contexte d'utilisation des données permet d'apprécier le risque d'atteinte aux libertés de l'individu concerné par celles-ci (46). En effet, la donnée en tant que telle représente rarement un danger pour l'individu. C'est son utilisation qui crée le risque d'atteinte à la personne. Que l'on sache qu'une personne est un homme ou une femme est *a priori* anodin et sans danger. Mais cette donnée si elle est considérée comme critère prépondérant dans un traitement ayant pour finalité l'analyse du risque d'insolvabilité acquiert une portée qui n'est plus neutre et qui peut être à la base d'une discrimination injustifiable.

(46) Voir CNIL, *Dix ans d'informatique et libertés*, Economica, 1988, pp. 36 et 42.

37. C'est pourquoi les législations « privacy » ont fondé leur protection sur le principe dit « de finalité ». Celui-ci implique que le but du traitement soit déclaré et déterminé. Cela permet de vérifier la compatibilité de l'utilisation des données avec cette finalité. La finalité déclarée détermine donc les limites d'utilisation des données à caractère personnel dans le chef du responsable du traitement.

38. Toute finalité n'est cependant pas acceptable. Les textes « privacy » posent le principe selon lequel, pour être admise, la finalité déclarée doit être légitime. Ainsi en est-il lorsque la Convention n° 108 du Conseil de l'Europe déclare en son article 5 b. que les données à caractère personnel sont « enregistrées pour des finalités déterminées et légitimes ». Pour plus de clarté nous parlerons dans la suite du texte de « principe de légitimité ». Mais une finalité légitime n'autorise pas d'elle-même l'utilisation de n'importe quelle donnée. Pour pouvoir être traitées en vue d'une finalité légitime, les données doivent présenter un lien étroit avec celle-ci. On ne pourrait, par exemple, accepter qu'une donnée concernant la religion ou une condamnation pénale soit traitée pour apprécier la capacité de remboursement d'un demandeur d'un crédit. C'est pourquoi les législations « privacy » n'autorisent un traitement que si les données sont pertinentes, adéquates et non excessives par rapport à la finalité légitimement déterminée. C'est cette triple exigence que nous proposons de regrouper sous le vocable (47) de « principe de conformité » (48).

39. Le problème est alors de cerner la portée exacte de ce double principe : légitimité d'une part, conformité d'autre part.

(47) Il n'existe pas, en effet, de concept qui vise de lui-même cette triple exigence.

(48) Ces deux principes, consacrés formellement dans la Convention n° 108 du Conseil de l'Europe, se retrouvent aujourd'hui dans la plupart des législations « privacy ». Voir par exemple l'article 5 du projet de loi belge (Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. parl.*, Sén., sess. extr., 1991-1992, n° 445-1.) ; art. 4 et 5 de la loi néerlandaise (Wet van 28 december 1988, houdende regels ter bescherming van de persoonlijke levensfeer in verband met persoonsregistraties, *Staatsblad*, 1988, 665) ; art. 16.1 b et c de la proposition de Directive (Proposition de Directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel, COM (90), 314 final, septembre 1990, pp. 48 et svtes). Ce dernier texte vient d'être modifié pour tenir compte des nombreux amendements proposés par le Parlement européen. Il n'est pas encore officiel. D'après nos renseignement, les principes de légitimité et de conformité ont été repris et précisés sans remettre en cause nos présentes réflexions.

En effet, à partir de quel moment peut-on dire qu'une finalité est légitime ? Comment apprécier le caractère adéquat, pertinent et non excessif d'une donnée ? Les textes restent sans réponse.

Ici encore selon nous, la méthode de pondération des intérêts offre aux autorités de contrôle des critères d'évaluation qui permettent de donner un contour plus précis aux principes de légitimité et de conformité.

40. Conformité et légitimité doivent être clairement distinguées. Partons d'un exemple. Le ministère de l'enseignement envisage de commercialiser des données à caractère personnel concernant la population scolaire, collectées par les établissements qu'il contrôle. Cette commercialisation représente pour elle une finalité particulière. Pour satisfaire les exigences des principes de légitimité et de conformité, deux examens doivent être effectués. Le premier porte sur la légitimité. On s'interroge alors sur l'admissibilité de la mise sur pied d'un tel traitement par le ministère de l'enseignement. En prenant en considération le fait que la transmission des données est obligatoire dans le chef des étudiants, que la vente des données n'entre pas, à proprement parler, dans sa mission d'intérêt général, etc., peut-on accepter qu'il décide de son propre chef de transmettre, contre finances, des données antérieurement collectées pour un tout autre but ? Le second examen, celui de la conformité, vise à déterminer quelles données peuvent faire l'objet de ces transmissions eu égard à leur nature et aux risques spécifiques qu'une telle utilisation engendre dans le chef de la personne concernée.

Le traitement de données à caractère personnel suscite une opposition d'intérêts entre les personnes concernées par les données et celles qui les traitent. La seule possibilité de circonscrire les limites de l'utilisation des données, concrétisées par les principes de légitimité et de conformité, est d'équilibrer les intérêts en conflit. Ces deux principes ont dès lors un même objectif : l'équilibre des intérêts. Les autorités de contrôle peuvent utiliser une méthode de vérification : la méthode de pondération des intérêts.

Si l'on revient à notre exemple, en ce qui concerne la légitimité, il faudra vérifier si la commercialisation des données est utile et nécessaire au ministère de l'enseignement compte tenu des missions qui lui sont propres et qui lui sont prescrites par

la loi. Ensuite, on devra se demander si la brèche qu'elle ouvre dans l'intimité des personnes est proportionnée par rapport à l'intérêt général que l'administration prétend servir. Le lecteur imaginera sans difficulté des situations où le doute est permis. Ainsi, lorsque le but recherché par l'administration est purement financier sans que l'on puisse prétendre que la commercialisation se fait dans l'intérêt de la scolarité. En ce qui concerne la conformité, il faudra vérifier dans un premier temps si la transmission de chacune des données est utile et nécessaire eu égard à cette commercialisation supposée alors légitime. Dans un second temps, il faudra déterminer si la transmission de cette donnée n'entraîne pas une atteinte excessive vis-à-vis de l'avantage d'une telle commercialisation.

41. Si les principes de légitimité et de conformité participent tous deux à une recherche d'équilibre, leur contenu diffère cependant quelque peu.

1° Pour circonscrire les finalités légitimes d'un traitement, il faut, nous semble-t-il, respecter *deux grandes règles*. La première est formelle en ce sens qu'elle est sans rapport avec le choix effectué par le responsable du traitement. Elle prescrit tout d'abord que la détermination des finalités appartient exclusivement à une « autorité » déterminée par ou en vertu de la loi. Elle impose ensuite que les finalités soient définies de manière claire et précise. Ces exigences visent tant la protection de l'individu que la sécurité juridique. En effet, comment effectuer un contrôle efficace de la finalité (en ce compris la conformité) si celle-ci n'est pas connue ou est ambiguë ? La désignation d'un responsable par ou en vertu de la loi garantit quant à elle l'applicabilité de la sanction en cas de manquement.

La seconde règle a trait au fond. C'est ici que la méthode de pondération des intérêts trouvera à s'appliquer. Elle suppose que le choix de la finalité s'effectue dans le respect du point d'équilibre entre d'une part l'intérêt du responsable du traitement et, d'autre part, les intérêts des personnes concernées par les données.

2° Le principe de conformité, quant à lui, prescrit directement cette pondération des intérêts. Les trois critères retenus — l'adéquation, la pertinence et le caractère non excessif — correspondent très exactement au triple examen de la règle de propor-

tionnalité (utilité, nécessité, proportionnalité). La pondération se situe alors à un autre niveau que celle effectuée lors du *choix de la finalité*. Elle s'effectue ici lors du *choix des données* qui vont être traitées.

42. Le contrôle de la finalité implique ainsi une double analyse. La première porte sur la légitimité de la (des) finalité(s) déterminée(s) par le responsable ou par la loi au nom d'une liberté ou d'un intérêt. La seconde vise à s'assurer de la conformité des données à caractère personnel avec la réalisation de ces finalités. On verra que ce double contrôle doit très exactement s'effectuer par le biais de la méthode de proportionnalité afin de pondérer les intérêts en présence.

2° *Illustrations*

α Le contrôle de la légitimité

43. Dans le *secteur public*, la finalité du traitement sera légitime si elle répond aux trois principes de légalité, de spécialité et de proportionnalité (*supra*, n° 15). Le principe de légalité garantit le respect de la règle formelle : le législateur est l'autorité compétente pour déterminer les finalités. Les principes de spécialité et de proportionnalité permettront quant à eux de garantir la règle de fond (l'équilibre des intérêts). Les finalités doivent donc entrer dans le cadre des missions spécifiques confiées à l'autorité publique au sein de laquelle le traitement sera mis sur pied. Elles doivent de plus être nécessaires au regard de l'intérêt général ou de la protection des citoyens sans pour autant qu'elles n'engendrent une atteinte disproportionnée par rapport à ce but.

Prenons un exemple classique : la commercialisation par le ministère des communications ou des transports des données à caractère personnel contenues dans les répertoires des immatriculations automobiles.

En France, la C.N.I.L. (49) a admis que le répertoire serve non seulement à assurer la sécurité routière mais également la promotion du secteur automobile autorisant ainsi la commercialisation du fichier auprès des entreprises de ce secteur mais non par exemple du secteur du marketing direct. La justification de cette solution reste assez vague (50). La question du principe de légalité est restée sous silence. Selon la C.N.I.L., la fourniture des données aux constructeurs français et à certains importateurs rencontre l'intérêt général « en assurant la promotion d'un secteur clé de l'économie nationale ». Mais ne pourrait-on justifier de la même façon la transmission des données au secteur du marketing qui est aussi un secteur économique important ? Les exigences de motivation résultant de l'application du contrôle de légitimité permettrait d'éviter le flou d'une telle solution.

Quant à la République fédérale d'Allemagne (51), elle restreint à la seule finalité « sécurité routière » les communications du répertoire. La réglementation est claire sur ce point. Seules les administrations de la gendarmerie, de la justice et autres ont droit à la communication ; les entreprises d'assurances ne peuvent les réclamer que dans l'hypothèse de litiges précis. Les exemples français et allemand mettent en évidence deux façons différentes de déterminer la frontière à partir de laquelle la poursuite de l'intérêt général doit s'effacer devant les libertés individuelles.

A notre avis, une correcte application du principe de légitimité doit permettre une approche rationnelle du problème. Il faut d'abord se demander si le ministère est habilité à poursuivre une telle finalité en vertu d'une loi et si sa mise en œuvre telle que proposée rentre bien dans ce cadre légal (règle formelle). Il faut ensuite soumettre cette finalité à la règle de fond du principe de légitimité. Le but de la commercialisation est-il nécessaire au vu des missions d'intérêt général poursuivies par une telle administration ? La mise en œuvre de l'intérêt général n'entraîne-t-elle pas une limitation disproportionnée des libertés individuelles ?

(49) CNIL, *4e rapport d'activités*. Doc. Fr., Paris, 1984, pp. 87 et 309.

(50) Voir J. HUET et H. MAISL, *Droit de l'informatique et des télécommunications*, Litec, Paris, 1989, p. 583, n° 543.

(51) Dans ce pays, les registres d'immatriculation automobile sont réglementés par la Strassenverkehrsgesetz (*BGBl*, I, 1987, 487) et le Fahrzeugregisterverordnung (*BGBl*, I, 1987, 2305). Sur tout cela, cfr l'étude *Publaw* réalisée pour le compte de la Commission européenne (DG XIII) par le Centre de Recherches Informatique et Droit de Namur, le G.M.D. de Köln et le Center for Information Law de la London University, étude en voie de publication.

On voit que le contrôle de légitimité par la méthode de pondération des intérêts est particulièrement adapté au secteur public. Les principes de spécialité et de proportionnalité — à la base de toute l'action administrative — se confondent ici avec la règle de proportionnalité au sens large décrite ci-avant (52).

44. En ce qui concerne le *secteur privé,* on retrouve, *mutatis mutandis*, les mêmes critères d'appréciation.

La *règle formelle* est ici garantie par le fait que les lois « privacy » désignent généralement le responsable du fichier comme celui qui détermine les finalités du traitement (53). De plus, cette finalité étant portée à la connaissance de l'individu concerné, de l'autorité de contrôle et, le cas échéant, du public, elle devra être déterminée avec clarté et exactitude (54).

La *règle de fond* se retrouve également dans le secteur privé. Les responsables de fichier invoqueront ici leur liberté contractuelle, d'entreprendre, d'expression ou un autre intérêt afin de légitimer leur ingérence dans la sphère de liberté de la personne concernée par les données. Toutefois, ces libertés ou intérêts ne sont pas sans limites. Il faudra donc contrôler si la finalité du traitement ne déborde pas du cadre du contrat passé avec l'individu et/ou si elle relève bien de la liberté d'entreprendre ou de tout autre intérêt invoqué par le responsable du fichier. Il faudra également vérifier que la finalité du traitement n'implique pas une ingérence disproportionnée dans la vie privée de l'individu même si elle doit être jugée nécessaire quant au but poursuivi.

45. D'aucuns riquent d'être étonnés de l'application du principe de légitimité dans le secteur privé (55). Mais, on l'a vu, les

(52) Le principe de légalité implique que l'illégitimité qui trouve sa source dans une loi ne pourrait être parfaitement sanctionnée que par une cour constitutionnelle, la sanction résidant alors généralement dans l'annulation de l'acte législatif ou de la disposition en cause. On trouve un bon exemple de ce contrôle dans l'affaire du recensement démographique portée devant le Tribunal constitutionnel fédéral allemand (voir *supra*).

(53) Voir par exemple l'article 1, § 6, du projet de loi belge ; art. 2.e de la proposition de Directive européenne ; art. 2.d de la Convention n° 108 du Conseil de l'Europe.

(54) Cette exigence fait l'objet d'un contrôle particulier de la C.N.I.L. Voir CNIL, *Dix ans d'informatique et libertés, op. cit.*, p. 37 ; J. FRAYSSINET, *Informatique, fichiers et libertés-les règles, les sanctions, la doctrine de la C.N.I.L.*, Paris, Litec, 1992, p. 73, n° 170.

(55) Voir P. GLINEUR, *Droit et éthique de l'informatique*, Story-Scientia, 1991, n°s 192 et suivants. D'après cet auteur, seul le principe de conformité permettrait un contrôle des fichiers du secteur privé.

lois « privacy » stipulent explicitement le respect du principe de légitimité sans limiter son champ d'application à tel ou tel secteur. Ceci n'implique ni une négation de la liberté d'entreprendre, ni un frein au marché de l'information. Il s'agit seulement de s'assurer que l'exercice des libertés invoquées par les responsables de traitement, s'exprimant par le choix d'une finalité, respecte celles des personnes concernées. Nous ne sommes dès lors pas dans le domaine du principe de conformité. Deux exemples permettront de le comprendre. Le premier concerne le marketing direct ; le second vise la communication des données.

— Les firmes spécialisées dans le marketing direct ont pour but de permettre une publicité efficace de tel ou tel produit en ciblant soigneusement ses destinataires. Une entreprise d'automobiles de haut de gamme désire lancer une campagne de publicité en envoyant un catalogue « toutes boîtes ». Elle s'adresse à une société de marketing afin de se limiter aux destinataires qui, théoriquement, peuvent être intéressés par ce type de véhicule. Pour ce faire, l'entreprise de marketing rassemble et traite un nombre considérable de données à caractère personnel en vue d'établir un profil très précis des personnes concernées. Cette finalité purement mercantile soulève la question de sa légitimité. Dans son 10e rapport d'activité (56), la C.N.I.L. a très bien cerné cette problématique : « Le problème que pose cette activité économique (le marketing direct) qui répond elle-même à un besoin économique, est de savoir dans quelles conditions elle doit être exercée pour ne pas être ressentie comme une agression et une atteinte à la vie privée. En d'autres termes, il s'agit de trouver un compromis acceptable entre des impératifs commerciaux de plus en plus forts et le droit d'être laissé tranquille reconnu par la loi ». Mais comment atteindre ce compromis et sanctionner, le cas échéant, sa violation, si ce n'est par le biais de la méthode de pondération des intérêts usitée lors du contrôle du respect du principe de légitimité ? En matière de marketing direct, la finalité n'est pas *a priori* illégitime. Elle ne le sera que si sa mise en œuvre entraîne une rupture de l'équi-

(56) CNIL, *10e rapport d'activités-1989*, Doc. Fr., Paris, 1990, pp. 9 et 10.

libre des intérêts en présence (57). On voit donc bien que la solution n'est pas à trouver dans le principe de conformité mais bien dans celui de la légitimité tel qu'explicité plus haut. Il est à noter que les tests de l'utilité et de la nécessité se concluront généralement de façon positive. Le problème est de déterminer à partir de quel moment ce type de finalité engendre une violation inacceptable des droits de la personne.

— Le lien existant entre la communication — opération particulière sur des données à caractère personnel — et la finalité d'un traitement se présente de deux manières différentes.

Dans un premier cas, la communication constitue véritablement une des finalités d'un traitement. Ainsi, des données à caractère personnel éparpillées au sein d'une grande base de données se verront rassemblées et classées afin d'être revendues à des tiers, une société de mailing par exemple. Cette commercialisation constitue une communication particulière en ce sens qu'elle est effectuée dans le seul but d'en tirer un profit financier. La communication est ici recherchée pour elle-même et représente la finalité de ce genre de traitement. Elle suscite les questions suivantes :

1° Quelle est l'origine des données ? Dans quel cadre et dans quel but ont-elles été rassemblées ?

2° A qui les données sont-elles transmises ? Que va-t-on en faire ?

Dans un second cas, la communication des données est nécessaire à l'accomplissement d'une finalité distincte. Une banque, en vue d'effectuer un payement international, transmet différentes données à une consœur étrangère pour les besoins de l'opération. La finalité du traitement est ici de gérer le service proposé à la clientèle, à savoir le suivi de leurs opérations de compte. Les questions se posent alors différemment :

1° La communication se justifie-t-elle au regard de la finalité poursuivie ?

(57) Voir par exemple sur ce point J. HUET et H. MAISL, *Droit de l'informatique et des télécommunications*, Litec, Paris, 1989, p. 221, n° 248 ; J.-Ph. WALTER, « Recommandation n° R (85) 20 du Comité des ministres du Conseil de l'Europe relative à la protection des données à caractère personnel utilisées à des fins de marketing direct », in *XIII^e Conférence des Commissaires à la Protection des données (2-4 octobre 1991)*, Conseil de l'Europe, Strasbourg, 1992, pp. 128 à 149.

2° Y a-t-il un risque de réutilisation en vue de l'accomplissement d'une autre finalité dans le chef du destinataire ?

Dans ces deux hypothèses, les risques engendrés pour la personne concernée par les données se situent d'une part en amont, dans le chef de l'émetteur des données (questions 1° : l'entreprise qui vend les données ; la première banque) et d'autre part en aval, dans le chef du destinataire des données (questions 2° : l'entreprise de mailing ; la seconde banque).

Ces transmissions de données représentent toujours un danger potentiel pour l'individu. Des communications successives provoquent en effet un éparpillement des données qui rend très difficile le contrôle de leur utilisation ultérieure par la personne concernée. Ici encore, l'application correcte du principe de légitimité permettra d'éviter un certain nombre de difficultés et de clarifier des situations parfois complexes. Cette application fera l'objet d'un double contrôle. Le premier s'effectuera dans le chef de l'émetteur des données, le second dans celui du récepteur.

Du fait de la relation particulière qu'il entretient avec la personne concernée par les données, l'émetteur peut se voir interdire toute communication de données qui s'effectuerait en dehors de la finalité d'utilisation prévue sous peine de rompre le lien de confiance qui les unit. Il en est ainsi lorsqu'une obligation de discrétion ou de secret professionnel régit un secteur particulier. On pense naturellement au secteur bancaire ou médical. Ainsi, une communication de données effectuée par une banque ne peut être autorisée que si elle est nécessaire au service proposé à la personne concernée et pour autant qu'elle n'implique pas une violation excessive des libertés de celle-ci. On le voit, la communication — qu'elle représente la finalité d'un traitement à part entière ou qu'elle participe à une autre finalité — implique que cette finalité soit confrontée à la règle de fond du principe de légitimité. Seule une pondération d'intérêts permet alors de trouver une solution.

En l'absence d'un tel lien existant entre la personne concernée et l'émetteur des données, le contrôle du principe de légitimité s'effectue également. Dans l'hypothèse où la communication constitue une finalité en soi (exemple de la vente à l'entreprise de mailing), il s'agira de vérifier si la communication est utile

et nécessaire à l'exercice des libertés invoquées par le responsable du traitement et si elle n'énerve pas exagérément celles de la personne concernée. Dans l'hypothèse où la communication participe à une autre finalité, il faudra se poser la question de l'utilité et de la nécessité de cette communication en fonction de ce but et vérifier qu'elle n'engendre pas un risque disproportionné quant aux libertés de la personne concernée.

Cependant, ce contrôle « à la source » ne rend pas *ipso facto* toute transmission légitime. Le récepteur des données à caractère personnel doit lui aussi satisfaire au principe de légitimité. La communication n'est pas une opération neutre. Elle comporte intrinsèquement un risque d'atteinte à la vie privée puisque de ce fait un plus grand nombre de personnes prend connaissance des données. Ce risque justifie en soi que la communication ne puisse avoir lieu que si elle satisfait un intérêt légitime du destinataire des données. Cette condition ne s'oppose d'ailleurs pas à la libre circulation de l'information. Elle est au contraire à la source de la recherche d'équilibre qui seul permet de la rendre acceptable (58).

Si la communication constitue le but même du traitement, l'utilisation ultérieure des données par le destinataire devra faire l'objet d'un contrôle de légitimité. Dans le cas de la vente des données à une entreprise de mailing, les finalités déclarées par cette dernière, comme leur mise en œuvre, devront être respectueuses des libertés individuelles (voir *supra*, nos réflexions concernant le marketing direct). Elles se doivent donc d'être utiles et nécessaires et ne peuvent engendrer une atteinte excessive dans le chef des personnes concernées. On retrouve la méthode de pondération des intérêts décrite plus haut (59). Si la communication s'intègre dans une autre finalité, la gestion des opérations de compte par exemple, le traitement effectué par le destinataire des données ne posera plus de problème de légitimité tant qu'il conserve le même but. La difficulté est alors de savoir si le destinataire peut traiter les données selon une finalité différente de celle qui présidait à la transmission. La banque

(58) Voir les considérants 2 et suivants de la proposition de Directive européenne.

(59) Il est à noter que la loi allemande qui, à notre sens, effectue l'application la plus correcte du principe de légitimité, prévoit explicitement ce contrôle dans le chef du destinataire des données (art. 29 (2) 1.a, Federal Data Protection Act).

réceptrice des données peut-elle conserver ces données pour une période qui excède les besoins de l'opération de payement et les traiter pour son propre compte ? Le principe de finalité s'y oppose. Mais on pourrait imaginer que ces données soient intégrées dans un traitement dont la finalité soit elle-même déclarée et légitime. La solution est alors plutôt à trouver dans le principe de conformité qui a pour objet le lien entre les données et la finalité.

46. Ainsi compris, le principe de légitimité apparaît, tous secteurs confondus, comme le premier rempart de l'individu face à un usage abusif de traitements qui impliquent en dernière analyse une atteinte inacceptable à la liberté de la vie privée. Il faut cependant remarquer que s'il peut faire l'objet d'un contrôle en ce qui concerne les finalités qui font l'objet d'un libre choix par les autorités qui y sont spécialement habilitées par la loi (responsable du traitement ou législateur), il donne également une assise théorique solide à certaines dispositions légales ou réglementaires venant entraver *a priori* l'action des exploitants de fichiers.

Ainsi en est-il de l'article 2, al. 1^er^, de la loi française qui interdit que l'on prenne des décisions de justice sur base d'un traitement donnant une définition du profil ou de la personnalité de l'individu. Une telle disposition se fonde sur la croyance que dans l'hypothèse de décisions de justice entièrement automatisées, le point d'équilibre entre les intérêts en présence est forcément rompu au détriment de l'individu.

Autre exemple : les restrictions *a priori* de la communication des données. On ne peut admettre que n'importe qui ait accès aux données à caractère personnel qui sont traitées. Dans certains cas, une loi définit précisément quelles sont les personnes qui y sont habilitées. En Belgique, la nouvelle loi sur le crédit à la consommation détermine (60) une liste limitative des personnes ou organismes qui pourront se voir communiquer les données concernant les mauvais payeurs. Une telle disposition a été justifiée explicitement par référence à l'intérêt légitime des

(60) Article 69, § 4, de la loi du 12 juin 1991 relative au crédit à la consommation, *M.B.*, 9 juillet 1991, pp. 15203 et svtes, modifiée par la loi du 6 juillet 1992, *M.B.*, 9 juillet 1992, pp. 15 728 à 15 730.

destinataires potentiels de ces données (61). Peu importe ici le caractère plus ou moins complet de cette liste, l'important est de relever que cette interdiction est basée sur l'idée selon laquelle toute autre communication est censée *ipso facto* entraîner une ingérence excessive dans la vie privée des personnes concernées.

Le principe de légitimité peut enfin fonder des décisions de l'autorité de contrôle qui viennent modaliser la mise en œuvre de certaines finalités. On en trouve un exemple en France dans une décision de la C.N.I.L. (62) qui n'admet la commercialisation de l'annuaire des P.T.T. que sous certaines conditions (existence d'une liste orange, information accrue de l'individu etc.). A nouveau, le raisonnement qui sous-tend une telle décision est à trouver dans le principe de légitimité. Si les conditions ne sont pas remplies, une telle finalité risque en de nombreux cas de provoquer une rupture d'équilibre entre les intérêts en présence.

47. Les virtualités du principe de légitimité ne semblent pas encore avoir été complètement exploitées. Une affaire soumise à la C.N.I.L. en 1990 (63) paraît révélatrice du peu d'intérêt qui lui est accordé tant par la doctrine que par les autorités de contrôle.

En 1981, un groupement de sociétés d'assurances déclare à la C.N.I.L. un traitement automatisé de données dont la finalité principale est le recensement et la diffusion de données relatives aux assurés présentant un risque particulier de surmortalité. Reprenant plus de 300 000 noms, il vise, par une meilleure information des compagnies, à éviter les fraudes ou erreurs des assurables. Suite à une visite de contrôle, la C.N.I.L. découvre diverses irrégularités. Sa délibération ne fut pas suivie d'effets. Suite à une demande du Conseil national du sida, la C.N.I.L. procède alors à une nouvelle réévaluation du fichier. L'épidémie de sida engendrant une inquiétude de la part des assureurs, le

(61) La motivation de l'élargissement de cette liste qui a eu lieu via la loi du 6 juillet 1992 se concentre très exactement sur la description de l'intérêt des personnes ou organismes qui pourront également dans l'avenir accéder aux données (voir Commentaires des articles, art. 3, *Doc. parl.*, Ch., sess. extr., 1991-1992, pp. 4 et svtes).

(62) Voir la délibération n° 85-22 du 18 juin 1985 citée in LAMY, « Droit de l'informatique », *Accès aux données à caractère personnel*, Lamy, Paris, 1992, n°s 1186 et références.

(63) Voir la délibération n°s 90-95 du 11 septembre 1990 relative au fichier des risques aggravés vie in *11ème rapport d'activité de la C.N.I.L.*, La documentation française, Paris, 1991, pp. 153 et svtes.

fichier pouvait servir à exclure les personnes malades ou même séropositives du champ de l'assurance. Lors de sa délibération du 11 septembre 1990, la C.N.I.L. remarque que le fichier présente un risque d'illicéité en vertu de l'article 2 de la loi française en ce qu'il pourrait générer des décisions automatiques de rejet des demandeurs. Mais elle va plus loin dans son raisonnement. Elle remarque, en vertu de ce que nous avons appelé la règle de la proportionnalité (*supra*, n° 30), que ce fichier n'est pas indispensable à l'appréciation du risque présenté par un client. En effet, chaque compagnie a la possibilité de faire procéder à un examen médical. Elle va jusqu'à déclarer « que l'existence (du fichier) paraît au demeurant contestable ». De là à dire que la finalité du fichier est illégitime, il n'y a qu'un pas. En effet, en estimant que d'autres méthodes, à savoir l'examen par chaque société des cas qui se présentaient, permettaient aux sociétés d'assurances de prévenir le risque, la C.N.I.L. admet que ce risque est alors légitimement combattu sans que soit nécessaire la création d'un fichier commun qui, s'il répondait bien à la même finalité, créait un danger disproportionné d'atteinte aux libertés des citoyens (64). Le contrôle révèle donc un manquement au principe de légitimité, ce qui rend le traitement illicite au regard de l'article 5 b de la Convention n° 108 du Conseil de l'Europe.

β Le contrôle de la conformité

48. Pour que le traitement d'une donnée à caractère personnel réponde au principe général de conformité, trois conditions doivent être remplies : elle doit être adéquate, pertinente et non excessive par rapport à la finalité du traitement qui lui sera (est) appliqué (cfr *supra*, n°s 39 et svts).

L'adéquation et la pertinence doivent ici se comprendre comme impliquant une liaison nécessaire et suffisante de la donnée ou de la catégorie de données à la finalité en cause. Prenons par exemple un traitement visant l'évaluation de la capacité de remboursement d'un prêt bancaire. Pour un client adulte, le montant de ses revenus professionnels constitue une donnée

(64) *In casu*, la C.N.I.L. s'est bornée à prescrire quelques conseils au cas où le fichier serait maintenu. Finalement, le groupement a décidé de supprimer ledit fichier.

adéquate et pertinente. Par contre, les revenus de ses parents présentent un lien trop lâche avec cette finalité. La situation serait différente si ceux-ci se portaient cautions de leur enfant. Si la banque exigeait de plus le numéro d'identification des personnes physiques afin d'identifier le client, cette donnée serait considérée comme non pertinente et inadéquate ; la banque peut en effet s'assurer de l'identité par d'autres moyens qui diminueront le risque d'atteinte à la vie privée de la personne concernée. Les données à caractère personnel récoltées par la banque doivent de plus être non excessives par rapport à la finalité d'évaluation de la solvabilité et ce, même si elles apparaissent nécessaires. Ainsi, pourrait-on peut-être affirmer statistiquement que telle ou telle tranche de clientèle appartenant à une catégorie de population (immigré, indigène, ouvrier, cadre, etc.) est plus dépensière que d'autres. Le problème est alors de savoir si l'utilisation de telles données n'entraîne pas une intrusion disproportionnée dans la vie privée des personnes concernées.

49. On voit très bien que le contrôle de conformité doit lui aussi s'effectuer à travers une méthode de pondération des intérêts. Les trois étapes du raisonnement (utilité, nécessité, proportionnalité) se retrouvent d'ailleurs explicitement dans le principe de conformité. La C.N.I.L. contrôle depuis toujours le principe de pertinence par cette voie (65). La législation allemande, quant à elle, reprend le principe de pertinence directement sous la forme d'une pondération à rechercher via la règle de proportionnalité (66).

50. Rappelons enfin que tout comme en matière de légitimité, la pondération des intérêts, sous-jacente au principe de conformité, peut être effectuée *a priori* par la législation. Ainsi la loi française (67) interdit-elle notamment que les données faisant apparaître les origines raciales d'un individu fassent l'objet d'une conservation dans une mémoire informatisée sauf accord exprès de l'intéressé (68). Cette disposition se fonde ici encore

(65) Voir A. LUCAS, *op. cit.*, pp. 91 et 92, n° 83. L'auteur y affirme avec raison que le principe de proportionnalité apparaît dans ce cas comme un corollaire du principe de finalité. Pour des exemples d'applications, voir *11e rapport d'activité de la C.N.I.L.*, *op. cit.*, pp. 179, 191 et 300.

(66) Voir art. 14 (1) et 28 (1), 2 du Federal Data Protection Act.

(67) Article 31, al. 1.

(68) Sur la portée du consentement, voir *infra*, (d).

sur le présupposé selon lequel la conservation d'une telle donnée entraîne en elle-même une atteinte injustifiée aux droits de la personne par le risque de discrimination qu'elle porte en elle et ce, indépendamment de la finalité invoquée.

b) *La relative distinction entre secteur privé et secteur public*

51. Les principes de légitimité et de conformité s'appliquent tant au secteur public qu'au secteur privé. Pour ce qui est de la conformité, cette double application est entièrement vérifiée. C'est une évidence lorsque la législation s'applique sans distinction aux deux secteurs (69). De plus, les textes « privacy » qui font la distinction le prévoient dans des dispositions communes aux deux secteurs (70). L'explication est à trouver dans le fait que le principe de finalité est à la base de la protection et ce, indépendamment du secteur en cause.

En ce qui concerne la légitimité, son application aux deux secteurs est bien réelle même si l'approche présente des spécificités dues à l'organisation différente de ceux-ci. Seul le principe de légalité est réellement l'apanage du secteur public. Il se comprend aisément si l'on rappelle que le traitement de données à caractère personnel doit alors être compris comme l'accessoire de l'action administrative en général. Les autorités administratives ne pouvant rien faire, sauf ce que la loi leur permet (71), il est normal que ce principe s'applique également lorsqu'elles traitent des données à caractère personnel.

Les principes de spécialité et de proportionnalité s'expliquent de la même manière. Il faut remarquer que ces deux principes se retrouvent *mutatis mutandis* dans le secteur privé. Comme l'autorité administrative ne peut enregistrer des données que dans le cadre de la mission qui lui a été confiée, elle-même rele-

(69) Ainsi l'article 5.c de la Convention n° 108. Voir aussi l'article 5 du projet de loi belge.

(70) Ainsi l'article 16.c de la proposition de Directive européenne. En France où la loi ne prévoit pas explicitement le principe de pertinence, la C.N.I.L. l'applique sans distinction aux deux secteurs (voir A. LUCAS, *Droit de l'informatique*, P.U.F., Coll. Thémis, 1987, p. 91, n°s 83 et svts). Cela peut paraître moins évident en Allemagne car le texte exprime le principe de manière quelque peu différente. Il se voit dans les deux cas traduit explicitement par le principe de proportionnalité tout en étant « adapté » au secteur en cause. Une analyse approfondie de la législation permet cependant de dire qu'il s'applique dans les deux secteurs quoique assorti d'exceptions différentes (voir les articles 13.1 et 14.1 pour le secteur public et les articles 28 (1), 1 et 2, 29 et 30 du Federal Data Protection Act (1991).

(71) Voir P. GLINEUR, *op. cit.*, pp. 111 et svtes et références citées.

vant de l'intérêt général ou de la protection d'intérêts individuels (principe de spécialité), le responsable du fichier ne peut traiter des données qui sont sans rapport avec les finalités qu'il se choisit en rapport avec l'objet social de son entreprise et qui matérialisent l'intérêt ou la liberté qu'il invoque. De même, si les finalités d'un traitement dans le secteur public doivent se limiter à ce qui est nécessaire et proportionné par rapport à l'intérêt général ou à la protection des intérêts des citoyens (principe de proportionnalité), nous avons vu que la même restriction existe dans le secteur privé relativement aux libertés ou intérêts invoqués.

On peut donc dire que le régime de protection des données est l'émanation de principes communs trouvant à s'appliquer de manière analogue dans les deux secteurs. C'est seulement au niveau de la mise en œuvre des principes de légitimité et de pertinence que peuvent apparaître des règles différentes dans ces deux secteurs.

c) *Le consentement de la personne concernée*

52. Quelle portée peut avoir le consentement de l'intéressé dans l'appréciation des exigences découlant des principes de légitimité et de conformité ? Le rôle du consentement dans les législations « Informatique et libertés » est assez ambigu. Deux positions extrêmes s'opposent. D'aucuns pensent que la personne concernée par les données est bien souvent en position de dépendance vis-à-vis du ficheur. Le consentement préalable de la personne concernée est alors artificiel puisqu'il donne l'illusion d'un choix qui n'existe pas (72). Les autres partent du principe que la personne concernée par les données est toujours à même de jauger son intérêt de manière éclairée. Par conséquent, elle peut permettre toute utilisation déclarée de données qui la concernent.

La vérité est sans doute médiane. Certes, dira-t-on, l'individu peut comprendre très facilement où se situe son avantage. C'est à lui à déterminer le seuil de risque au-delà duquel il refuse le traitement et ce, en fonction de l'avantage qu'il obtiendra en

(72) Voir F. RIGAUX, *op. cit.*, n° 540. Sur la portée du consentement en général en matière de vie privée, voir n°s 685 et svts. Voir aussi *supra*, *Sixième leçon : La distinction entre les droits subjectifs patrimoniaux et les biens non patrimoniaux*, n°s 151 et svts.

retour. Mais sa volonté de l'obtenir peut l'inciter à des concessions dont il ne mesure absolument pas les conséquences. Pour se voir accorder un crédit, il acceptera de légitimer la vente ultérieure des données susceptibles de refléter sa capacité de remboursement. *Exit*, le secret bancaire ? *Exit* aussi, une attente légitime quant à la discrétion ? Tout cela au nom d'une acceptation qui, dans de nombreux cas, pourrait être obtenue par manipulation, fût-elle indirecte. Pour éviter tout excès, il paraît nécessaire de réserver à l'autorité de contrôle une possibilité de « neutraliser » le consentement de l'individu en cas d'abus. De plus, des garanties doivent être prévues *a priori* afin de s'assurer que le choix de la personne est suffisamment éclairé. C'est dans ce sens qu'il faut comprendre l'exigence d'un consentement exprès (73) ou informé (74) de l'individu.

53. Le consentement de l'individu peut recevoir deux portées différentes selon les textes en vigueur. Il permet au responsable du fichier soit de traiter certaines données considérées comme sensibles (75), soit de légitimer les finalités d'un traitement (76).

Lorsqu'il porte sur l'autorisation de traiter certaines données sensibles, le consentement se situe au niveau de l'application du principe de conformité. La personne accepte l'utilisation de certaines données pour une finalité déterminée qui lui est clairement explicitée. Une personne autorise par exemple une banque à enregistrer des données relatives aux résultats obtenus lors de ses études ou à son état de santé alors que ce n'est pas strictement pertinent quant à la finalité du traitement (l'analyse de sa solvabilité, par exemple). Une autre consent à des examens cliniques complémentaires, ce qui engendre une collecte de nouvelles données en vue d'une recherche médicale n'ayant rien à voir avec sa maladie. Dans ces cas, un contrôle reste possible par le biais du principe de légitimité. La finalité pour laquelle ces données seront utilisées doit respecter l'équilibre des intérêts

(73) Voir la doctrine française à ce sujet in LAMY, « Droit de l'informatique », *Accès aux données à caractère personnel*, Lamy, Paris, 1992, n° 1179 et références citées.

(74) Voir l'article 12 de la proposition de Directive européenne.

(75) Voir l'article 31 de la loi française ; art. 7, al. 2, du projet de loi belge (données médicales).

(76) Voir les articles 5 b et 8.1 de la proposition de Directive et l'article 4 (1) de la loi allemande.

en cause. La liberté d'entreprendre y trouve son compte mais son exercice abusif peut être sanctionné.

54. Le consentement qui porte sur la légitimité est, à notre sens, plus problématique. La proposition de directive européenne déclare clairement qu'un traitement est légitime s'il est couvert par le consentement de la personne concernée par les données (77). Il faudrait en conclure que des finalités présentant clairement des risques d'atteinte disproportionnée, voire des finalités injustifiables selon le service rendu ou la mission poursuivie, se retrouvent en quelque sorte exclus de tout contrôle parce que le traitement en question est opéré sous le couvert du consentement de l'individu. On a vu que la légitimité se trouve au centre d'un débat de société. Elle pose le problème de la valeur de l'individu face à des intérêts qui le dépassent. Accepter qu'il légitime lui-même l'utilisation des données qui lui est décrite, revient à nier cette dernière difficulté.

L'importance du débat engendré dans nos sociétés par l'utilisation de traitements de données à caractère personnel explique que l'on ait ressenti le besoin de créer une autorité indépendante des parties aux fins de contrôle non seulement du respect des lois de protection — ce qui équivaut à un contrôle de licéité au sens strict — mais aussi, et surtout, afin d'apprécier, loin de tout débat passionnel, les besoins et les intérêts des parties en présence. Accepter que le consentement rende légitime toute utilisation des données à caractère personnel reviendrait à réduire à néant cet acquis. En cas de consentement de la personne concernée, l'autorité de contrôle verrait son pouvoir gravement amputé car, même en cas d'abus manifeste, elle ne pourrait que s'incliner.

55. C'est pourquoi nous ne pouvons accepter que le consentement couvre la légitimité du traitement. Le consentement exprès et informé peut s'analyser en un contrat par lequel une personne permet à l'autre d'utiliser les données qui la concernent dans un but prédéfini. Il faut considérer la pondération des intérêts, garantie notamment par le principe de légitimité comme un principe d'ordre public qui ne souffre aucune exception basée sur la liberté contractuelle. Puisque bien souvent les

(77) Articles 5 b et 8.1.

parties ne sont pas sur un pied d'égalité, le principe de légitimité permet de contrer toute pratique consistant à extirper un consentement en cas de déséquilibre manifeste des intérêts en présence.

56. Le consentement exprès et informé permet de traiter certaines données sensibles. Il autorise aussi des traitements de données pour des finalités « inhabituelles ». Ainsi, est laissée à l'autorité de contrôle, le cas échéant au juge, la possibilité d'exercer leur mission de contrôle de légitimité. Dès que le traitement des données sensibles ou les buts dans lesquels certains traitements sont effectués s'avèrent impliquer une ingérence inacceptable, fût-ce sous le couvert du consentement de la personne, l'autorité doit soit pouvoir frapper le traitement d'illégitimité, soit ordonner que des mesures particulières soient prises afin de rééquilibrer les intérêts en présence (78).

Conclusions

57. Nos réflexions n'avaient d'autres buts que d'explorer les perspectives ouvertes par les thèses du professeur Rigaux dans le débat dit « Informatique et vie privée ». Cette analyse nous est apparue féconde à plus d'un titre.

La thèse de M. Rigaux abolit définitivement toute idée d'une « vie privée » en soi aux contours définis et conçue sur le mode d'une propriété. Elle invite à un débat plus essentiel, plus complexe et plus vivant qui renvoie la question de la protection des données à un nécessaire arbitrage entre libertés. En quittant le domaine de la propriété, le débat sur la protection des données a perdu ses certitudes, celle d'une vie privée bien circonscrite, celle de finalités décrites une fois pour toutes ; en entrant dans le domaine des libertés, il a gagné en inquiétudes, non celles, paralysantes, conduisant au refus du progrès technique, mais bien celles, mobilisatrices, invitant à entamer en des lieux divers

(78) *Contra* : Proposition de Directive (*op. cit*) ; voir aussi la Recommandation n° R (91) 10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics. Selon cette dernière, la communication de données du secteur public au secteur privé n'est pas forcément soumise au principe de légalité ; le consentement de la personne suffit normalement à légitimer celle-ci (art. 2.1. d), sauf en ce qui concerne les données sensibles (art. 3.1.). Il va de soi que notre thèse y est totalement opposée. Il revient au lecteur de se ranger derrière l'une ou l'autre de ces solutions.

une discussion fondée sur la transparence des enjeux de la technologie informationnelle, et ce, afin que s'élaborent de véritables choix.

Ces choix nécessitent une juste pondération des intérêts qui demande que soient pesés en *toute transparence* les intérêts des uns à « connaître », des autres, à échapper à cette connaissance ; en d'autres termes, elle exige un contrôle des finalités des traitements de données. La règle de proportionnalité offre à ce débat une méthode qui oblige le contrôleur à systématiser son raisonnement dans la clarté, étant entendu que le dernier mot restera toujours une décision libre.

58. L'examen de la finalité d'un traitement soulève d'abord la question de sa légitimité tant formelle que de fond. Légitimité formelle, il s'agit de désigner l'autorité compétente et responsable pour la définition de la finalité. Légitimité de fond, il s'agit de choisir une finalité compatible avec la liberté ou l'intérêt que l'on invoque tout en respectant les libertés individuelles des personnes concernées par les données. Le débat est loin d'être purement conceptuel. Il peut amener une comparaison des techniques de traitements utilisées au regard des craintes suscitées à l'égard des libertés individuelles et entraîne, selon les cultures de chaque pays, des choix qui peuvent être différents selon leur sensibilité.

Cet examen de légitimité se double d'un examen de la conformité des données par rapport aux finalités du traitement. Il s'agit cette fois de limiter le contenu des traitements et des communications aux seules informations nécessaires à l'exécution des missions légitimes de celui qui réclame le droit à l'information.

59. La distinction « légitimité du traitement » et « conformité des données » apparaît utile notamment pour comprendre la portée du consentement du fiché. Si celui-ci peut librement décider d'élargir le droit à l'investigation de l'entreprise ou de l'administration, ce consentement ne dispense pas de maintenir le traitement dans le cadre des finalités légitimes poursuivies par cette entreprise ou cette administration.

Cette distinction doit valoir tant pour le secteur privé que public. Même si les critères de légitimité et de conformité peuvent connaître dans l'un et l'autre cas des contraintes différentes, leur examen doit y être effectué également.

60. « Informatique et libertés », c'est bien de libertés au pluriel qu'il faut parler, de libertés dont il faut *pondérer les intérêts respectifs* avant de trancher en faveur de l'une ou de l'autre.

La tâche n'est pas aisée. Elle est exigeante parce qu'elle engage des choix sur la manière dont une société veut vivre parce qu'elle réclame la clarté des débats et la rigueur de l'analyse. C'est aux autorités de protection des données que revient en premier lieu ce lourd devoir. Elles ne l'accompliront que dans la mesure où s'institue dans les divers lieux de décision et de vie une véritable préoccupation, non celle frileuse de la vie privée à protéger, mais celle plus enthousiaste de libertés à conquérir.

Dans cette réflexion, l'outil technologique n'est pas un ennemi mais, le cas échéant, un moyen au service d'un vouloir vivre ensemble.

Thierry LÉONARD — Yves POULLET